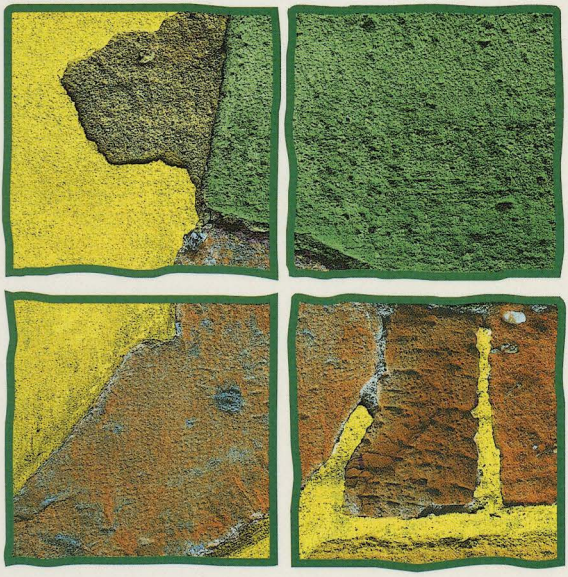
Schriftenreihe des
Instituts für Rechtswissenschaft
und Rechtspraxis

Universität St.Gallen

Ueli Kieser / Kurt Pärli (Hrsg.)

Datenschutz im Arbeits-, Versicherungs- und Sozialbereich: Aktuelle Herausforderungen



Band 80

Ueli Kieser / Kurt Pärli

(Herausgeber)

Datenschutz im Arbeits-, Versicherungs- und Sozialbereich: Aktuelle Herausforderungen

mit Beiträgen von

Dr. iur. Bruno Baeriswyl
Matthias Horschik, Rechtsanwalt
PD Dr. iur. Ueli Kieser
Prof. FH Peter Mösch Payot, lic. iur. LL.M.
Prof. Dr. iur. Kurt Pärli
lic. iur./exec. MBA HSG Ursula Uttinger

Referate der Tagung vom 29. November 2011 in Luzern

St. Gallen 2012

Inhaltsübersicht

Evaluieren, kontrollieren, überwachen: Datenschutz in Arbeitsverhältnissen

Prof. Dr. iur. KURT PÄRLI, PD für Arbeits- und Sozialversicherungsrecht an der Universität St. Gallen, Leiter Zentrum für Sozialrecht, School of Management and Law, Zürcher Hochschule für angewandte Wissenschaften, Winterthur

Inhaltsübersicht

I) Einleitung

1. Die Überwachung von Arbeitnehmenden im Zeitalter von PC und Internet

Die Überwachung von Beschäftigten ist kein neues Phänomen. Die Sklaven wurden durch Aufseher kontrolliert und mit Peitschenhieben zur Arbeit angehalten. In den Büros früherer Zeiten verfolgte der Bürovorstand von seinem erhöhten Pult aus die Aktivitäten der Bürolistinnen und Bürolisten. Heute stehen den Unternehmen zahlreiche technische Überwachungsmöglichkeiten zur Verfügung.

Besonders zentral ist die Überwachung im Zusammenhang mit den heute wohl wichtigsten Arbeitsinstrumenten, PC und Internet. Die Betriebssysteme und Anwendungsprogramme an sich haben bereits Funktionen eingebaut, die es Interessierten möglich machen, zahlreiche Informationen über die Nutzer/innen und deren Surf- und e-Mail-Verhalten zu gewinnen. Log-Protokolle dienen der rationellen Verarbeitung der gewonnenen Informationen. Sogenannte Cookies legen Informationen aus dem Internet auf dem lokalen PC ab. Zu erwähnen ist weiter der "Cache", ein Verzeichnis auf dem PC oder in Firmennetzwerken, in dem die Inhalte der besuchten Internetseiten zwischengespeichert werden. Log-Protokolle, Cookies und Cache sind Fundgruben für die Erkennung des individuellen Surfverhaltens. Das Kontrollpotential bei der elektronischen Kommunikation ist immens. Überwacht werden kann nicht nur jede Form der e-Mail-Kommunikation, eine Kontroll- und Überwachungsfunktion haben auch Proxy-Server, Fernwartungszugriffe oder Formen der Desktopüberwachung[1].

Ebenfalls zur Überwachung von Arbeitnehmenden eingesetzt werden können neuere Technologien wie die "Radio-Frequency-Identification" (RFID), die ein berührungsloses Auslegen von sogenannten "Tags" z.B. in Auswei-

1 Einen guten Überblick über heute gängige Kontrollmöglichkeiten der Aktivitäten der Arbeitnehmer/innen am PC und im Internet bietet der folgende Beitrag: GERRIT WIEGAND/JENS MÖSINGER, Der Chef surft mit – Technische Möglichkeiten der Mitarbeiterinnen- und Mitarbeiter-Kontrolle bei der Internet- und E-Mail Nutzung und wie man sich davor schützen kann, 2008, siehe: http://www.onlinerechte-fuer-beschaeftigte.de/upload/s480e1c9f6be9d_verweis1.pdf (besucht: 1.5.2012).

sen, Schlüsseln oder in der Kleidung ermöglicht. Jeder dieser "Tags" hat eine eindeutige Nummer und allenfalls weitere Daten. RFID wird bspw. für die Zeiterfassung oder das Öffnen von Türen eingesetzt. Mitarbeitende können ferner via GPS oder Handy geortet werden[2].

Angeboten werden auf dem Markt auch spezielle Überwachungsprogramme zur Überwachung von Mitarbeitenden in Echtzeit. So wirbt z.B. die Firma "refog" für ihre Überwachungssoftware: "Nutzt die Personal-Überwachung Ihrer Firma was? Nutzen all Ihre Mitarbeiter die PCs und Internet ausschliesslich für Geschäftszwecke? Arbeiten sie gleich fleissig, egal, ob Sie über ihre Schulter schauen oder ausserhalb des Büros sind? In anderen Wörtern – zweifeln Sie manchmal deren Produktivität an? Sie sollten daran denken, ein Überwachungssystem zu installieren, um sich mit dem Problem zu befassen. Überwachung in Echtzeit ist notwendig, um Mitarbeiter-Produktivität zu erhöhen, jedoch löst sie nicht das Problem der Mitarbeiter-Loyalität"[3]. Der Einsatz der Refog-Software, so wirbt das Unternehmen weiter, sei für das Personal komplett unsichtbar und insbesondere könnten auch die Kommunikation der Mitarbeitenden in "Social Networks" kontrolliert werden. Ähnliche Produkte bietet auch eine Firma mit dem sinnigen Namen "Orvell Network" an[4]. Automatisches Monitoring von Facebook- und Twitter-Aktivitäten der Mitarbeitenden verspricht das Produkt von "teneros.com"[5].

Nicht alles, was technisch möglich ist, ist in rechtlicher Hinsicht auch erlaubt; die folgenden Ausführungen setzen sich mit dem rechtlichen Rahmen auseinander. Daten- und persönlichkeitsschutzrechtliche Bestimmungen und Bestimmungen im Arbeitsgesetz setzen der Überwachung und Kontrol-

---

2 Zu den Möglichkeiten und Grenzen der Ortung von Mitarbeitenden siehe die aktuelle Studie der TA Swiss (Technology Assessment): LORENZ HILTY, BRITTA OERTEL, MICHAELA WÖLK, KURT PÄRLI, Lokalisiert und identifiziert, Wie Ortungstechnologien unser Leben verändern, siehe: http://www.vdf.ethz.ch/service/3460/3477_Lokalisiert-und-identifiziert_OA.pdf (besucht: 16.5.2012).

3 http://www.refog.de (besucht: 1.5.2012).

4 http://www.protectcom.de/orvell/netzwerk.php (besucht: 1.5.2012).

5 http://www.teneros.com (besucht am: 1.5.2012).

le der Mitarbeitenden Grenzen (III) und beschränken bereits die zulässige Datenbearbeitung im Bewerbungsprozess (II). Für die Arbeitgeberseite besteht regelmässig die Problematik, dass sie die Arbeitnehmer/innen nicht nur aus purem Eigeninteresse überwachen wollen, vielmehr sind sie aus rechtlichen Gründen, Sicherheit oder Compliance-Regelungen rechtlich dazu verpflichtet. Es eröffnen sich hier Spannungsfelder und Widersprüche zwischen Compliance-Durchsetzung und Datenschutz (IV). Der Beitrag wird mit einem Fazit und weiterführenden Überlegungen abgeschlossen (V).

II) Eignungsabklärung der Arbeitnehmenden

1. Der rechtliche Rahmen

Datenschutz ist nicht Selbstzweck. Es sind nicht die Daten, die geschützt werden müssen; Sinn und Zweck des Datenschutzes ist vielmehr der Schutz der Persönlichkeit von Personen, über die Daten bearbeitet werden. Dieser Grundgedanke zeigt sich in der verfassungs- und menschenrechtlichen Verankerung des Datenschutzes. In der Bundesverfassung (BV) bestimmt Art. 13 Abs. 2 den Anspruch jeder Person "auf Schutz vor Missbrauch ihrer persönlichen Daten". Weiter garantiert Art. 8 Abs. 1 EMRK jeder Person das Recht auf Achtung ihres Privatlebens (u.a.), und der Europäische Gerichtshof für Menschenrechte hat wiederholt erkannt, dass darunter auch ein Anspruch auf Schutz vor missbräuchlicher Datenbearbeitung zu verstehen ist[6]. Auch in der Grundrechtscharta der Europäischen Union (GRCh) findet sich eine eigenständige Bestimmung zum Grundrecht auf Datenschutz (Art. 8 GRCh[7]). Zum übergeordneten rechtlichen Rahmen gehören ferner die Da-

6 Siehe z.B. EGMR, Urt. v. 6.9.1978, X ./. Vereinigtes Königreich, und in jüngerer Zeit EGMR, Urt. v. 17.7.2008, I. ./. Finnland, Nr. 20511/03.

7 Nach Art. 8 Abs.1 GRCh hat jede Person Anspruch auf Schutz der sie betreffenden personenbezogenen Daten und Abs. 2 legt bereits auf Grundrechtsstufe Bearbeitungsgrundsätze fest (Bearbeitung nach Treu und Glauben, Einwilligung, Auskunftsrecht).

tenschutzkonvention des Europarates[8] und die Datenschutzrichtlinie der Europäischen Union[9]. Letztere ist für die Schweiz auch als Nicht-EU-Mitglied insofern relevant, als die Richtlinie vorschreibt, dass Daten nur in Staaten mit einem vergleichbaren Datenschutzniveau transferiert werden dürfen[10]. Im Ergebnis muss deshalb schweizerisches Datenschutzrecht den EU-rechtlichen Schutzansprüchen entsprechen[11].

Dem Anspruch auf Schutz von Personendaten, vorliegend der Schutz von Personendaten der Arbeitnehmer/innen, stehen regelmässig divergierende Interessen gegenüber. Vorliegend sind dies die Arbeitgeberinteressen an möglichst umfassenden Informationen über die Arbeitnehmer/innen bezüglich deren fachlichen und persönlichen Eignung für die Einstellung oder Beförderung. Auf grundrechtlicher Ebene sind die Arbeitgeberinteressen im Grundrecht auf Wirtschaftsfreiheit, das auch die Vertragsfreiheit umfasst, geschützt[12].

Die Konkretisierung des Datenschutzes auf Gesetzesstufe erfolgt auf sämtlichen staatlichen Ebenen und in verschiedenen Rechtsgebieten[13]. Für private Arbeitsverhältnisse massgebend sind zum einen das Bundesgesetz über den Datenschutz (DSG) und zum anderen Art. 328b OR als datenschutzrechtliche Spezialnorm im Arbeitsvertragsrecht. Nach Art. 328b OR darf die Ar-

---

8 Konvention Nr. 108 zum Schutz des Einzelnen im Hinblick auf die automatische Verarbeitung von personenbezogenen Daten, Europäische Datenschutzkonvention, DSK, SR 0.235.1.

9 Datenschutzrichtlinie 95/46/EG vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

10 Siehe Art. 25 und 26 der Rl 95/46/EG.

11 FRANK SEETHALER, N 78 ff., Entstehungsgeschichte des DSG, in: Maurer-Lambrou/Vogt (Hrsg.), Datenschutzgesetz, 2. Auflage, Basel 2006, S. 26 ff.

12 Zur Vertragsfreiheit als Teil der Wirtschaftsfreiheit von Art. 27 BV siehe statt vieler: KLAUS VALLENDER, N 37 zu Art. 27 BV, in: Ehrenzeller/Mastronardi/Schweizer/Vallender (Hrsg.), Die schweizerische Bundesverfassung, Kommentar, 2. Auflage, Basel/Zürich/St. Gallen 2008.

13 EVA MARIA BELSER/HUSSEIN NOUREDDINE, Datenschutzgesetz des Bundes, in: Belser/Epiney/Waldmann (Hrsg.), Datenschutzrecht – Grundlagen und öffentliches Recht, Bern 2011, S. 412 f.

beitgeberin Personendaten des Arbeitnehmers nur bearbeiten, "soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind". In Art. 328b Satz 2 OR wird darauf hingewiesen, dass im Übrigen die Bestimmungen des DSG gelten.

Mit der Beschränkung der zulässigen Bearbeitung von Arbeitnehmerdaten auf die Eignungsabklärung und auf solche Arbeitnehmerdaten, die zur Durchführung des Arbeitsvertrages notwendig sind, konkretisiert der Gesetzgeber das in Art. 4 DSG verankerte Verhältnismässigkeitsprinzip, gegenüber dem DSG wird der Schutz im Arbeitsverhältnis durch Art. 328b OR erhöht[14], was der Prämisse des Arbeitsrechts Rechnung trägt, wonach die Arbeitnehmenden als schwächere Vertragspartei zu schützen sind. Trotz ihrer systematischen Stellung im Vertragsrecht ist unbestritten, dass Art. 328b OR bereits im Bewerbungsverfahren Anwendung findet[15]. Im Bewerbungsverfahren sind zudem die weiteren Bearbeitungsgrundsätze des DSG wie das Prinzip der Rechtmässigkeit der Datenbearbeitung (Art. 4 Abs. 1 DSG), das Zweckbindungsgebot (Art. 4 Abs. 3 DSG), der Transparenzgrundsatz (Art. 4 Abs. 4 DSG), aber auch das Gebot der Datenrichtigkeit (Art. 5 DSG) zu beachten. Besondere Beachtung erfordert der im Zuge der ersten Revision des DSG im Jahre 2008 neu eingeführte Art. 4 Abs. 5 DSG: "Ist für die Bearbeitung von Personendaten die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung erst gültig, wenn sie nach angemessener Information freiwillig erfolgt. Bei der Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen muss die Einwilligung zudem ausdrücklich erfolgen". Im arbeitsrechtlichen Zusammenhang bedeutet dies, dass bei Referenzauskünften (hier werden regelmässig besonders schützenswerte Personendaten bearbeitet), die Bewerber/innen ihre ausdrückliche Zustimmung erteilen müssen. Das blosse Erwähnen früherer Arbeitgeber dürfte dafür nicht ausreichen[16].

---

14 So auch DAVID ROSENTHAL, N 1 zu Art. 328b, in: David Rosenthal/Yvonne Jöhri, Handkommentar zum Datenschutzgesetz, Zürich/Basel/Genf 2008.

15 ROGER RUDOLPH, Stellenbewerbung und Datenschutz, Bern 1997, S. 18 ff.

16 ROGER RUDOLPH, Das revidierte Datenschutzgesetz im arbeitsrechtlichen Fokus: eine Übersicht, ARV online 2008, Nr. 153.

Art. 328b OR erlaubt wie dargestellt die Datenbearbeitung aus zwei Gründen, Eignungsabklärung einerseits und Durchführung des Arbeitsverhältnisses andererseits. Diese beiden erlaubten Bearbeitungszwecke sind klar auseinanderzuhalten. So sind für die Arbeitgeberin gewisse, auch heikle Personendaten für die Durchführung des Arbeitsverhältnisses notwendig, etwa die Anzahl der Kinder, der Familienstand (wegen der Leistungspflicht für Kinder- und Familienzulagen) oder die Gewerkschaftszugehörigkeit[17] (um festzustellen, ob von einem Arbeitnehmer ein Solidaritätsbeitrag für die Durchführung des GAV vom Gehalt abzuziehen ist oder nicht). Auch die Information über den Bezug einer Teil-Invalidenrente ist bei Teilzeitbeschäftigten eine notwendige Information für die Durchführung des Arbeitsverhältnisses (wegen des entsprechend geringeren Koordinationsabzuges bei der beruflichen Vorsorge). Alle soeben genannten Personendaten sind aber regelmässig für die Eignungsabklärung erforderlich, könnten aber den Anstellungsentscheid der Arbeitgeberin unzulässigerweise beeinflussen (z.B. Nichtanstellung wegen der Anzahl Kinder eines Bewerbers oder des Vorliegens einer Teilinvalidität, letztere ist nicht per se aussagekräftig für die Arbeitsfähigkeit).

2. Ausgewählte Gerichtspraxis

In BGE 122 V 267 hatte das Eidg. Versicherungsgericht (EVG) in einer arbeitslosenversicherungsrechtlichen Sache über die Tragweite des Persönlichkeits- und Datenschutzes im Rahmen einer Stellenbewerbung zu befinden. In casu ging es um eine stellensuchende Versicherte, die sich weigerte, einen Personalfragebogen mit viel zu umfassenden Fragen vollständig auszufüllen. Der Fragebogen enthielt nicht bloss Fragen zu arbeits- oder arbeitsplatzspezifischen Sachverhalten, sondern auch ganz eindeutig solche mit persönlichkeitskennzeichnenden Merkmalen wie Freizeitverhalten und

17 Siehe dazu BGE 123 III 129: Der Arbeitgeber darf sich nach dem Abschluss des Arbeitsvertrags über die Gewerkschaftszugehörigkeit eines Arbeitnehmers erkundigen, um festzustellen, ob dessen Lohn nach den Vorschriften des vom Arbeitgeber unterzeichneten GAV festgesetzt werden muss (E. 3b/cc).

sonstiges Privatleben, die im Hinblick auf die fragliche Stelle ohne Belang waren. Für das EVG sind solche Fragen, insbesondere etwa diejenige nach dem Umgang mit inneren Problemen, Teil der schützenswerten Privatsphäre und somit unzulässig. Das EVG kam zum Schluss, der Versicherten könne daraus kein arbeitslosenversicherungsrechtlich relevantes Fehlverhalten vorgeworfen werden. Auch nicht vorgeworfen werden konnte der Versicherten, das sie sich nicht mit dem arbeitsrechtlichen Notwehrrecht der Lüge geholfen hatte (BGE 122 V 267, Erw. 4c).

Unzulässige Fragen der Arbeitgeberin bilden auch Hintergrund der Bundesgerichtsentscheidung vom 30. Juni 2008 (Urteil 2C_103/2008). Einer Stiftung im Kanton Waadt wurde die Bewilligung zur Ausbildung von Lehrlingen entzogen, nachdem bekannt geworden war, dass Vertreter der Stiftung bei den Bewerbungsgesprächen intime Fragen an die Bewerberinnen gerichtet hatten, u.a. bezüglich der von den Bewerberinnen angewendeten Empfängnisverhütungsmethoden. Solche Fragen sind gemäss Entscheid des Bundesgerichts selbst dann nicht zulässig, wenn es sich um einen Tendenzbetrieb handelt (die Stiftung bezweckt u.a. die Förderung der natürlichen Methode der Empfängnisverhütung mit Temperaturmessung und Schleimkontrolle). Das Urteil zeigt die Grenzen zulässiger Fragen in einem Tendenzbetrieb auf und macht deutlich, dass der Kernbereich der Persönlichkeit – und dazu gehört zweifellos die Form der Empfängnisverhütung – dem Informationshunger der Arbeitgeberin, auch wenn es sich um einen Tendenzbetrieb handelt, entzogen ist.

Die Grenzen des "Zugriffs" der Arbeitgeberin auf die Privatsphäre bildet weiter die Grundlage der Entscheidung der Eidg. Datenschutzkommission vom 29. April 2003. Die generelle Erhebung von Drogentests von sämtlichen Lehrlingen und Lehrtöchtern einer Firma bei Lehrbeginn und stichprobenweise zweimal pro Jahr während der Lehre ist eine widerrechtliche Datenbearbeitung, da es an einer freien Einwilligung der Betroffenen mangelt und sich das absolute Drogenverbot während der ganzen Lehre auch nicht durch arbeitsplatzbezogene Interessen rechtfertigen lässt. Die betroffene Arbeitgeberin begründete ihr Handeln mit der Fürsorgepflicht gegenüber den Auszubildenden. Die Eidg. Datenschutzkommission hielt dazu fest: "Das von

Roche verfolgte Ziel, ihren Auszubildenden eine drogenfreie Lehrzeit zu ermöglichen, soll hier vorerst nicht beurteilt werden. So achtenswert dieses Ziel auch ist, so stellt sich indessen die Frage nach der Verhältnismässigkeit der Massnahmen zur Erreichung dieses Ziels. Diese laufen darauf hinaus, die Fürsorgepflicht des Arbeitgebers auch auf das Privatleben der Auszubildenden auszudehnen; denn es ist davon auszugehen, dass z.B. gerade Cannabis vor allem ausserhalb der Arbeitszeiten konsumiert wird. Eine derartige Erweiterung des arbeitsrechtlichen Schutzbereichs über die Belange des Arbeitsplatzes hinaus ist jedoch dem schweizerischen Recht fremd. Gemäss Art. 328 Abs. 2 OR hat der Arbeitgeber zum Schutz von Leben, Gesundheit und persönlicher Integrität der Arbeitnehmerinnen und Arbeitnehmer die Massnahmen zu treffen, die nach der Erfahrung notwendig, nach dem Stand der Technik anwendbar und den Verhältnissen des Betriebes oder Haushaltes angemessen sind, soweit es mit Rücksicht auf das einzelne Arbeitsverhältnis und die Natur der Arbeitsleistung ihm billigerweise zugemutet werden kann (die Erwähnung des Haushaltes betrifft dabei einzig den Fall der Hausgemeinschaft). Die Lehre sieht in dieser Bestimmung vorwiegend eine *Begrenzung* der Schutzpflichten des Arbeitgebers und keineswegs eine Grundlage für deren Ausdehnung in die Privatsphäre der Angestellten (vgl. REHBINDER/PORTMANN, a.a.O., N. 9 f.)"[18].

Widerrechtlich ist nach einem Urteil des Bundesverwaltungsgerichts vom 14. Januar 2009 das Angebot einer privaten Firma eines umfassenden "Mitarbeiterchecks". Arbeitgeber konnten gegen Entgelt von dieser Firma umfassende Bonitätsauskünfte und weiter gehende Informationen über das persönliche Umfeld von Stellenbewerber/innen erhalten. Eine solche Datenbearbeitung fällt unter die erhöhten Anforderungen, die das DSG für die Bearbeitung von Persönlichkeitsprofilen stellt. Das bedeutet u.a., dass die Weitergabe an Dritte ohne besonderen Rechtfertigungsgrund widerrechtlich ist[19].

---

18 Urteil der Eidg. Datenschutzkommission vom 29. August 2003, Erw. 3.3.

19 Bundesverwaltungsgericht A-8028/2008 vom 14. Januar 2009.

3. (Un)zulässiges Online-Screening von Stellenbewerber/innen

Ist es zulässig, dass Unternehmen im Rahmen von Bewerbungsverfahren die Kandidatinnen und Kandidaten "googeln"? Gemäss einer Umfrage des Tages-Anzeigers ist diese Form der Beschaffung von Informationen über Bewerber/innen in einer Vielzahl von Betrieben absolut üblich[20]. Die Frage der rechtlichen Zulässigkeit musste bis heute noch nicht gerichtlich beurteilt werden. Auch die Datenschutzbehörden haben sich bislang zu dieser Problemstellung nicht geäussert. So fehlen z.B. auf den Merkblättern des Eidg. Daten- und Öffentlichkeitsbeauftragten (EDÖB) zum Datenschutz im Arbeitsverhältnis einschlägige Informationen[21].

In der juristischen Lehre hat sich URS EGLI in einer umfassenden Abhandlung zu "Sozialen Netzwerke(n) und Arbeitsverhältnis" auch mit dem "online-screening" von Bewerber/innen befasst[22]. EGLI weist vorerst darauf hin, dass eine Online-Recherche bei Google und anderen Suchdiensten sowie in sozialen Netzwerken wie Facebook Informationen zu Tage bringen kann, die von den betroffenen Personen nicht kontrolliert werden können. So ist bekannt, dass manchmal Informationen ohne Kenntnis oder sogar gegen den Willen der Betroffenen den Weg ins Netz finden. Google Earth und Google Street View ermöglichen zudem, sich anhand der in den Bewerbungsunterlagen vorzufindenden Adressangaben bereits ein Bild über den Wohnort der Bewerber/innen zu machen. EGLI erachtet ein allgemeines online-screening von Bewerber/innen als unzulässig: "Genauso wenig wie es zulässig wäre, sämtliche Bewerber systematisch und ohne deren Einverständnis durch Privatdetektive ausforschen zu lassen, ist es zulässig, sich selber im Internet als Detektiv zu betätigen"[23]. Zulässig ist eine Recherche im Internet dann, wenn in den Bewerbungsunterlagen ausdrücklich auf ein

---

20 http://www.tagesanzeiger.ch/leben/gesellschaft/Schweizer-Konzerne-ueberpruefen-Bewerber-im-Internet/story/17153295 (besucht: 15.5.2012).

21 Siehe zum Datenschutz im Arbeitsbereich auf der Internetseite des EDÖB: http://www.edoeb.admin.ch/themen/00794/00917/index.html?lang=de (besucht: 15.5.2012).

22 URS EGLI, Soziale Netzwerke und Arbeitsverhältnis – Über die Auswirkungen von Facebook, Xing & Co auf den betrieblichen Alltag, Jusletter vom 17. Januar 2011.

23 EGLI (Fn 22), Rz 79.

Profil in einem beruflichen Netzwerk hingewiesen wird und damit eine Einwilligung in die Datenbeschaffung und -bearbeitung vorliegt. Auch spezifische Sicherheitsbedürfnisse der Arbeitgeberin oder Compliance-Vorschriften rechtfertigen einen umfassenden "Backgroundcheck". Eine solche Sicherheitsprüfung ist indes dem Kandidaten oder der Kandidatin bekannt zu geben und es ist zudem die Gelegenheit zur Stellungnahme zu den Ergebnissen zu gewähren[24]. Verschiedene weitere Aspekte sind relevant: So muss die Arbeitgeberin die durch die Online-Recherche gewonnenen Informationen dokumentieren[25] und im Falle eines Auskunftsgesuches nach Art. 8 DSG der das Gesuch stellenden Person vollumfänglich Einsicht gewähren[26]. Weiter stellt sich das Problem, dass nicht auf die Eignung beschränkte Personendaten (siehe Art. 328b OR) für den Anstellungsentscheid gar nicht berücksichtigt werden dürfen[27].

Dass die Online-Recherche über Stellenbewerber/innen aus den dargelegten Gründen rechtlich in der Regel nicht zulässig sein dürfte, nützt den betroffenen Arbeitnehmer/innen wenig. Eine allfällige Datenschutzverletzung im Bewerbungsverfahren wird regelmässig schwierig zu beweisen sein. Wenn eine Anstellung infolge illegal erlangter und nicht die Eignung im Sinne von Art. 328b OR betreffenden Informationen über den Bewerber nicht zustande kommt, so stellt sich die Frage, welcher Schaden geltend gemacht werden könnte. Ein Anspruch auf Einstellung besteht nicht, so könnten lediglich die Bewerbungsunkosten und bei Vorliegen einer schweren Persönlichkeitsverletzung eine Genugtuung verlangt werden. Nur gerade im Anwendungsbereich des Gleichstellungsgesetzes (GlG) ist eine Pönalentschädigung für den Fall einer geschlechtsdiskriminierenden Nichtanstellung vorgesehen[28]. Einzig im Anwendungsbereich des GlG ist überdies die

24 EGLI (Fn 22), Rz 85.

25 EGLI (Fn 22), Rz 80.

26 Verstösse gegen das Auskunftsrecht, u.a. nicht vollständige Auskunftserteilung, werden nach Art. 34 DSG auf Antrag mit Haft oder Busse bestraft.

27 EGLI (Fn 22), Rz 84.

28 Art. 3 in Verbindung mit Art. 5 Abs. 2 GlG. Die Beweislasterleichterung nach Art. 6 GlG greift für Anstellungsdiskriminierungen nicht.

Möglichkeit vorgesehen, für eine Nichtanstellung eine Begründung zu verlangen[29].

4. Zwischenfazit

Als Zwischenfazit ist festzuhalten: Art. 328b OR und das DSG beschränken die zulässige Datenbeschaffung und -bearbeitung im Bewerbungsverfahren. Eine Datenbearbeitung ist nur zulässig für die Eignungsabklärung, wobei hier ein strenger, objektiver Massstab anzuwenden ist. Arbeitnehmerpersonendaten, die für die Durchführung des Arbeitsverhältnisses benötigt werden, dürfen nicht bereits im Bewerbungsverfahren erhoben werden, wenn dafür im Rahmen der Eignungsabklärung kein Bedarf besteht. Ein Blick auf die nicht sehr umfangreiche Gerichtspraxis zeigt, dass sowohl Art. 328b OR als auch das DSG dem überbordenden Informationshunger der Arbeitgebenden zum Schutz der Arbeitnehmenden Schranken setzen. Fraglich ist allerdings, ob das geltende Datenschutzrecht den neuen Bedrohungen der Arbeitnehmerpersönlichkeit vor dem Hintergrund der "schönen neuen Welt" des Internets genügt.

III) Kontrollieren und Überwachen

1. Rechtlicher Rahmen

1.1 Bestimmungen zum Schutze der Arbeitgeberinteressen und der Öffentlichkeit

In der Einleitung wurde auf die vielfältigen Überwachungsmöglichkeiten in der "schönen neuen Arbeitswelt" hingewiesen. Persönlichkeits- und Datenschutzbestimmmungen setzen der zulässigen Kontrolle und Überwachung der Arbeitnehmenden Schranken. Die Rechtsordnung gewährt indes auch der Arbeitgeberin rechtlichen Handlungsspielraum und auferlegt ihr sogar Pflichten zur Kontrolle und Überwachung der Arbeitnehmenden.

Ausgangspunkt bildet das für das Arbeitsverhältnis massgebende Unterordnungsverhältnis, welches im Weisungsrecht der Arbeitgeberin zum

29 Art. 8 Abs. 1 GlG.

Ausdruck kommt. Nach Art. 321d OR kann die Arbeitgeberin über die Ausführung der Arbeit und über das Verhalten im Betrieb allgemeine und individuelle Anordnungen erlassen. Es liegt auf der Hand, dass die Arbeitgeberin die Einhaltung ihrer Weisungen auch kontrollieren können soll. Die Arbeitgeberin haftet nach Art. 55 OR für den Schaden, den seine Hilfspersonen Dritten zufügen. Die Haftung entfällt nur, wenn die Arbeitgeberin nachweisen kann, dass sie ausreichend sorgfältig war, zu dieser Sorgfalt gehört auch die sachgerechte Kontrolle und Überwachung der Hilfspersonen[30].

Kontroll- und Überwachungspflichten ergeben sich vielfach auch aufgrund gesetzlicher Vorschriften, die den Interessen der Öffentlichkeit dienen. Zu denken ist an Sicherheitsvorschriften über den Umgang mit gefährlichen Materialien, an Bestimmungen zum Zwecke der Korruptions- oder Geldwäschereibekämpfung oder an das Wettbewerbsrecht. Weiter ergeben sich für die Arbeitgeberin aus der ihr obliegenden Fürsorgepflicht Pflichten, das Verhalten der Arbeitnehmenden untereinander im Betrieb so weit zu steuern, dass Mobbing, Diskriminierung und sexuelle Belästigung verhindert werden. Es liegt auf der Hand, dass die Arbeitgeberin auch hier die Einhaltung ihrer Weisungen kontrollieren können muss.

1.2 Bestimmungen zum Schutze der Arbeitnehmenden

Die Schranken der Überwachung der Arbeitnehmenden finden sich in der bereits weiter oben erläuterten arbeitsrechtlichen Datenschutzspezialnorm Art. 328b OR. Nur Arbeitnehmerdaten, die zur Eignungsabklärung (z.B. Abklärung der gesundheitlichen Eignung für eine bestimmte Tätigkeit) oder solche, die zur Durchführung des Arbeitsverhältnisses benötigt werden, dürfen bearbeitet werden, wobei bei der Bearbeitung auch die (weiteren) Bearbeitungsgrundsätze des DSG beachtet werden müssen. Basis der Schranken der Arbeitnehmerüberwachung bilden indes die allgemeine Persönlichkeitsschutznorm in Art. 328 OR und die öffentlichrechtliche Parallelnorm in Art. 6 Arbeitsgesetz (ArG).

---

30 THOMAS GEISER, Interne Untersuchungen des Arbeitgebers: Konsequenzen und Schranken, AJP 2011, S. 1047 ff.

Nach Art. 328 Abs. 1 OR hat die Arbeitgeberin im Arbeitsverhältnis die Persönlichkeit des Arbeitnehmers zu achten und zu schützen und auf dessen Gesundheit gebührend Rücksicht zu nehmen. Satz 2 von Art. 328 Abs. 1 OR verpflichtet die Arbeitgeberin überdies dazu, dafür zu sorgen, dass Arbeitnehmerinnen und Arbeitnehmer nicht sexuell belästigt werden und dass den Opfern von sexuellen Belästigungen keine weiteren Nachteile entstehen. Diese Verpflichtung zum Schutze der einen Arbeitnehmenden kann dazu führen, dass Massnahmen, auch solche der Kontrolle und Überwachung, gegenüber anderen Arbeitnehmenden ergriffen werden müssen. Auch dies hat indes wiederum in einem Rahmen zu erfolgen, der die Persönlichkeitsrechte der Überwachten und Kontrollierten nicht verletzt.

Art. 328 Abs. 2 OR und Art. 6 Abs. 1 ArG verpflichten die Arbeitgeberin zu Massnahmen zum Gesundheitsschutz der Arbeitnehmenden. Nach Art. 6 Abs. 2 ArG hat die Arbeitgeberin insbesondere "die betrieblichen Einrichtungen und den Arbeitsablauf so zu gestalten, dass Gesundheitsgefährdungen und Überbeanspruchungen der Arbeitnehmer nach Möglichkeit vermieden werden". Die Arbeitnehmenden sind gemäss Art. 6 Abs. 3 ArG für Fragen des Gesundheitsschutzes zur Mitwirkung heranzuziehen und sie (die Arbeitnehmenden) haben den Arbeitgeber in der Durchführung der Vorschriften über den Gesundheitsschutz zu unterstützen. Gestützt auf die Verordnungskompetenz in Art. 6 Abs. 4 ArG wurde die Verordnung 3 zum Arbeitsgesetz zur Gesundheitsvorsorge erlassen (ArGV 3). Vorliegend relevant ist Art. 26 ArGV 3, nach Abs. 1 dürfen Überwachungs- und Kontrollsysteme, die das Verhalten der Arbeitnehmer am Arbeitsplatz überwachen sollen, nicht eingesetzt werden, während Abs. 2 verlangt, dass Überwachungs- und Kontrollsysteme, die aus anderen Gründen erforderlich sind, so zu gestalten sind, dass die Gesundheit und die Bewegungsfreiheit der Arbeitnehmer nicht beeinträchtigt wird. Die Grenze zwischen unzulässiger reiner Verhaltensüberwachung und einer grundsätzlich zulässigen Überwachung aus anderen Gründen ist fliessend. Das seco erachtet in seiner Weisung zu Art. 26 ArGV 3 für die Abgrenzung zwischen unzulässiger und zulässiger Überwachung die folgenden Aspekte als massgebend: "Um zu wissen, ob die Einrichtung eines Überwachungsprozesses im Hinblick auf

Art. 26 ArGV 3 möglich ist oder nicht, muss abgeklärt werden, ob die drei nachstehenden Bedingungen erfüllt sind: Vorliegen eines anderen Interesses als die Verhaltensüberwachung der Arbeitnehmenden, Verhältnismässigkeit zwischen dem Interesse des Arbeitgebers an einer Überwachung und demjenigen der Arbeitnehmenden, nicht überwacht zu werden, Mitwirkung der Arbeitnehmenden bezüglich technische Einrichtung der Überwachung"[31].

Der Vollständigkeit halber ist noch auf den strafrechtlichen Schutz vor unbefugtem Beschaffen von Personendaten hinzuweisen. Zu nennen sind die Bestimmungen Art. 179bis ff. StGB, die strafbare Handlungen gegen den Geheim- oder Privatbereich enthalten. So wird z.B. nach Art. 179novies StGB auf Antrag mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft, wer unbefugt besonders schützenswerte Personendaten oder Persönlichkeitsprofile, die nicht frei zugänglich sind, aus einer Datensammlung beschafft. Weiter zu erwähnen ist das Fernmeldegeheimnis, auf das in Art. 43 und Art. 50 des Fernmeldegesetzes (FMG) hingewiesen wird.

2. Gerichtspraxis zu Video- und GPS-Überwachung

Leitentscheid zur GPS-Überwachung bildet BGE 130 II 425. Gemäss dieser Entscheidung ist der Einsatz eines GPS-Überwachungssystems dann zulässig, wenn dem Prinzip der Verhältnismässigkeit ausreichend Rechnung getragen wird. Von vornherein unverhältnismässig ist eine permanente Echtzeitüberwachung durch GPS, da diese dazu führen könnte, dass die Geschäftsleitung während der Dienstreise auch auf die Routenwahl der Mitarbeitenden einwirkt, was für die Betroffenen einen nicht akzeptierbaren Stress bedeute. Die GPS-Überwachung der Aussendienstmitarbeitenden war durch die Arbeitgeberin mit Argumenten begründet worden, von denen das Bundesgericht lediglich eines als mit dem Grundsatz der Verhältnismässigkeit vereinbar akzeptiert hat. Konkret hält das Bundesgericht fest, der Einsatz des GPS sei nicht geeignet als:

- Instrument der Diebstahlbekämpfung (weniger starke Eingriffe in die Persönlichkeit würden erlauben, ein gleiches Ergebnis zu erzielen),

31 Seco, Wegleitung zur Verordnung 3 zum Arbeitsgesetz, Art. 26 ArGV 3.

- zur Optimierung der Arbeitsorganisation (da die Echtzeit-Lokalisierung nicht erlaubt ist),
- zur Rationalisierung des Arbeitsablaufs für eine bessere Rechnungsstellung (die Arbeitgeberin konnte dieses Argument nicht begründen).

Das Bundesgericht kommt jedoch zum Schluss, der GPS-Einsatz sei erlaubt, soweit das Unternehmen dadurch überprüfe, ob die Mitarbeitenden tatsächlich beim Kunden seien[32].

Äusserst umstritten ist die Frage der Zulässigkeit der Videoüberwachung am Arbeitsplatz, da eine solche, besonders wenn permanent erfolgt, in hohem Ausmasse geeignet ist, bei den Überwachten Stress und Gesundheitsgefährdung hervorzurufen. Aus zwei neueren Bundesgerichtsurteilen lassen sich die Spielregeln für den Einsatz von Überwachungskameras ableiten.

Nach Ansicht der strafrechtlichen Abteilung des Bundesgerichts ist die Annahme des Verordnungsgebers in Art. 26 Abs. 1 ArGV 3, dass eine reine Verhaltensüberwachung per se die Gesundheit der Arbeitnehmenden gefährde und deshalb nicht erlaubt sei, falsch[33]. Hintergrund der Entscheidung vom 12. November 2009 bildet folgender Sachverhalt: In einer Bijouterie fehlte bei der täglichen Schlussabrechnung ein Betrag von 1350 Franken. Daraufhin konsultierte die Unternehmung die Aufnahmen der Kamera, die ohne Einwilligung und ohne Wissen der Angestellten im Kassenraum installiert war. Auf dem Film war eine Mitarbeiterin ersichtlich, die einen Bargeldbetrag aus der Kasse entnahm. Die Arbeitgeberin beschuldigte die Angestellte bei der Polizei des Diebstahls. Nach der Vorinstanz waren die Filmaufnahmen unrechtmässig (Verstoss gegen Art. 26 ArGV 3) erlangt worden und konnten deshalb im Strafprozess nicht als Beweismittel verwertet werden. Für das Bundesgericht ist fraglich, ob das in Art. 26 Abs. 1 ArGV 3 verankerte (absolute) Verbot der Verhaltensüberwachung (u.a.) durch Videoaufnahmen auf einer ausreichenden gesetzlichen Grundlage beruht. Das Arbeitsgesetz selbst enthalte keine Bestimmungen betreffend

32 BGE 130 II 425, Erw. 4 und Erw. 5. Kritisch zu den Schlussfolgerungen des Bundesgerichts: AMÉDÉO WERMELINGER, Digma 2/2005, S. 96 ff.

33 BGer 6B_536/2009 vom 12.11.2009.

Überwachung der Arbeitnehmer am Arbeitsplatz und auch keine entsprechende Delegationsnorm. Es erstaune, dass der heikle und schwierige Gegenstand der Überwachung der Arbeitnehmer am Arbeitsplatz lediglich in einer bundesrätlichen Verordnung geregelt sei[34].

Mit Blick auf die Entstehungsgeschichte, den systematischen Zusammenhang und die ratio legis von Art. 26 Abs. 1 ArGV 3 kommt das Bundesgericht zum Schluss, Überwachungs- und Kontrollsysteme, die das Verhalten der Arbeitnehmer überwachen sollen, dürften nur so weit nicht eingesetzt werden, wie sie die Gesundheit und das Wohlbefinden der Arbeitnehmer am Arbeitsplatz beeinträchtigten. Dem Verordnungsgeber könne nicht gefolgt werden, wenn er davon ausgehe, dass die Überwachung des Verhaltens in jedem Fall die Gesundheit der Arbeitnehmer beeinträchtige und deshalb zu verbieten sei[35]. Im vorliegenden Fall würden sich die Arbeitnehmer nur sporadisch und während kurzer Zeit im Kassenraum aufhalten. Eine solche Videoüberwachung sei nicht geeignet, die Gesundheit und das Wohlbefinden der Arbeitnehmer zu beeinträchtigen[36]. Weiter hält das Bundesgericht fest, angesichts der nur sporadischen und kurzzeitigen Überwachung und mit Blick auf das Interesse des Arbeitgebers an der Verhinderung von Straftaten durch Dritte würden durch die Videoüberwachung auch nicht die Bestimmungen zum Persönlichkeits- und Datenschutz des Arbeitnehmers am Arbeitsplatz verletzt[37]. Meines Erachtens verkennt das Bundesgericht hier die Bedeutung der auch für die Überwachung von Arbeitnehmenden anwendbaren Datenbearbeitungsgrundsätze des DSG. Die Beschaffung von Personendaten und der Zweck müssen für die betroffene Person erkennbar sein (Art. 4 Abs. 4 DSG). Zudem muss die Bearbeitung nach Treu und Glauben erfolgen und verhältnismässig sein (Art. 4 Abs. 2 DSG). Die Installation der Kamera an sich kann mit dem selbstverständlich legitimen Zweck des Schutzes vor Diebstahl gerechtfertigt werden. Die Nichtinforma-

34 BGer 6B_536/2009 vom 12.11.2009, Erw. 3.3.2.

35 BGer 6B_536/2009 vom 12.11.2009, Erw. 3.6.2.

36 BGer 6B_536/2009 vom 12.11.2009, Erw. 3.6.3.

37 BGer 6B_536/2009 vom 12.11.2009, Erw. 3.7.

tion über die Filmaufnahmen an die Arbeitnehmenden stellt indes eine Verletzung der erwähnten Datenschutzprinzipien dar. Der Schutz vor Diebstahl durch die Angestellten wird auch bei einer Information über die Kameraüberwachung erreicht. Eine transparente Kameraüberwachung stellt im Vergleich zu einer heimlichen Überwachung einen weitaus weniger gravierenden Eingriff in die Persönlichkeitsrechte der betroffenen Arbeitnehmenden dar. Zwar ist die Videoaufnahme ohne Information ein geeignetes Mittel zur Diebstahlsicherung, jedoch nicht erforderlich, da der Zweck auch bei vorgängiger Information des Personals erreicht wird[38].

Etwas anders gelagert war die Ausgangslage im Videoüberwachungsfall, den die sozialversicherungsrechtliche Abteilung des Bundesgerichts am 10. Juni 2011 zu entscheiden hatte[39]. Zu beurteilen war hier die Rechtmässigkeit einer Videoüberwachung, die ein vom Arbeitgeber nach konkretem Diebstahlsverdacht eingesetzter Privatdetektiv vorgenommen hatte. Die Staatsanwaltschaft des Kantons Basel-Landschaft stellte das Strafverfahren gegen den fraglichen Arbeitnehmer ein, da die Beweise im Sinne von Art. 26 Abs. 1 ArGV 3 widerrechtlich erlangt worden seien. Die Vorinstanz stellt sich auf den Standpunkt, auch im Sozialversicherungsrecht gelte grundsätzlich ein Verbot der Verwertung von rechtswidrig erlangtem Beweismaterial. Folglich dürfe die vorliegend involvierte Personalvorsorgeeinrichtung das Videomaterial nicht zur Beurteilung der Frage verwenden, ob der Versicherungsfall (die im Zuge der Verdächtigungen wegen Diebstahls eingetretene Invalidität) bei der Ausübung einer Straftat herbeigeführt worden sei. Das Bundesgericht kommt jedoch zum Schluss, eine Videoüberwachung, die erlaube, einen Verdächtigen zu überführen, sei, verhältnismässig angewendet, zulässig. Anders als bei präventiven Überwachungen müssten hier die Überwachten auch nicht vorgängig informiert werden, da dies ansonsten gerade den eigentlichen Überwachungszweck vereiteln würde[40].

---

38 Siehe hierzu: KURT PÄRLI, Urteil 6B_536/2009 der Strafrechtlichen Abteilung des Bundesgerichts vom 12. November 2009, Digma 2/2010, S. 76 ff.

39 BGer 9C_785/2010 vom 10. Juni 2011.

40 BGer 9C_785/2010 vom 10. Juni 2011, Erw. 6.7.

3. E-Mail, Internet, soziale Netzwerke

Für die Überwachung der E-Mail- und Internetaktivitäten sind die gleichen rechtlichen Rahmenbedingungen massgebend, die bereits weiter oben (1. Der rechtliche Rahmen) dargestellt wurden. Auch für den Europäischen Gerichtshof für Menschenrechte ist klar, dass e-Mail und Internet in den Schutzbereich von Art. 8 EMRK (Schutz des Privatlebens und der Korrespondenz) fallen[41].

In der Praxis kommt dem "Leitfaden des EDÖB über die Internet- und E-Mail-Überwachung am Arbeitsplatz" grosse Bedeutung zu[42]. Im Leitfaden wird zwischen präventiver Internet- und E-Mail-Überwachung und punktueller, personenbezogener Überwachung unterschieden. In einer ersten Phase (also bei der präventiven Überwachung) dürfen Logfiles ausschliesslich nicht personenbezogen ausgewertet werden. Nur beim Aufdecken eines Missbrauchs oder wenn ein konkreter Missbrauchstatbestand vorliegt, darf eine personenbezogene Auswertung der Logfiles vorgenommen werden[43]. Im Ergebnis ist es für einen Arbeitgeber rechtlich zulässig, die Einhaltung des Nutzungsreglements von Internet und E-Mail zu kontrollieren, sofern und soweit die Persönlichkeitsrechte der Arbeitnehmenden nicht verletzt werden. Unzulässig sind namentlich die ständige, namentliche Überwachung des Internet-Verhaltens oder der Einsatz von Spionage-Software-Programmen[44].

In der Praxis häufen sich Konstellationen, in denen Arbeitnehmende wegen Kritik am Arbeitgeber in "Social-Media"-Plattformen wie Facebook sanktioniert werden. So wurde bekannt, dass die Sicherheitsfirma "Delta" einen

---

41 Urteil der 4. Kammer des Europäischen Gerichtshofs für Menschenrechte vom 3. April 2007, Rechtssache Copland gegen U.K., Individualbeschwerde Nr. 62617/00, Rz 41.

42 Leitfaden über die Internet- und E-Mail-Überwachung am Arbeitsplatz, Eidg. Öffentlichkeits- und Datenschutzbeauftragter EDÖB, Bern, Juni 2009, http://www.edoeb.admin.ch/dokumentation/00445/00472/00532/index.html (besucht: 16.5.2012).

43 Leitfaden EDÖB (Fn 42), Kapitel 7 und 8, S. 18 ff.

44 Siehe zum Ganzen: GIORDANO COSTA, Internet- und E-Mail-Überwachung am Arbeitsplatz, Entwicklung in der Lehre, Rechtsprechung und Gesetzgebung, Jusletter vom 9. Januar 2012, Rz 31.

Mitarbeiter entliess, nachdem dieser auf Facebook damit prahlte, im Rahmen eines dienstlichen Einsatzes an einer Schlägerei teilgenommen zu haben[45]. Aufsehen erregte der Fall einer Kündigung an einer Arbeitnehmerin, die wegen Migräne zu Hause blieb und gleichzeitig Facebook besucht habe. Für die betroffene Arbeitnehmerin ist klar, dass die Arbeitgeberin sie auf Facebook mit einem falschen "Freund" ausspioniert habe[46]. In der Westschweiz wurde der Fall eines Buschauffeurs bekannt, der via SMS und via Facebook Arbeitskollegen/innen zu antikapitalistischen Aktionen aufgerufen hatte und sich auch über zu ängstliche Kollegen beklagte. Dem Chauffeur wird nun durch die Arbeitgeberin ein Fehlverhalten vorgeworfen und das Lausanner Arbeitsgericht wird zu entscheiden haben, ob die Äusserungen auf Facebook unter den Schutz der Privatsphäre des Arbeitnehmers fallen[47].

Arbeitsgerichtliche Urteile wegen Missachtung arbeitsvertraglicher Treuepflicht der Arbeitnehmer durch Aktivitäten in Social-Media-Plattformen sind in der Schweiz soweit ersichtlich noch keine ergangen. In Deutschland haben die Arbeitsgerichte mehrfach Beleidigungen gegenüber Chefs auf Facebook-Seiten von Angestellten nicht als Gründe für eine rechtmässige Kündigung anerkannt. So entschied das Arbeitsgericht Bochum, dass gegenüber Auszubildenden eine besondere Fürsorgepflicht bestehe, und auf dieser Basis dürfe ein Auszubildender nicht wegen Charakterisierungen des Vorgesetzten als "Menschenschinder" oder "Ausbeuter" entlassen werden[48]. Widerrechtlich war ferner die fristlose Entlassung einer Abteilungsdirektorin, nachdem deren Ehegatte sich auf Facebook kritisch gegenüber ihrer Arbeitgeberin geäussert hatte. Der Frau könne das Verhalten ihres Mannes nicht vorgeworfen werden, selbst wenn die Frau einen kritischen Kommentar auf Facebook abgegeben hätte, dürfe dies nicht überwertet werden, befand das Arbeitsgericht Dessau-Rosslau[49]. Auch mehrere französische Ge-

45 NZZ, 9.4.2010, S. 18.

46 20-Minuten online, 23. April 2009.

47 24heures, 11.04.2011.

48 ArbG Bochum, 29.03.2012 – 3 Ca 1283/11.

49 Arbeitsgericht Dessau-Roßlau, Urt. v. 21.03.2012 – Az.: 1 Ca 148/11.

richte mussten sich mit der Frage auseinandersetzen, ob negative Äusserungen von Arbeitnehmer/innen auf Facebook eine Arbeitgeberkündigung rechtfertigen. Rechtmässig war gemäss Urteil des Arbeitsgerichts Boulogne Billancourt vom 19. November 2010 die Entlassung dreier Mitarbeiter eines Unternehmens, nachdem sich diese auf Facebook kritisch zu ihrem Unternehmen geäusssert hatten[50].

4. Zwischenfazit

Die Arbeitgeberin ist zur Kontrolle und Überwachung der Arbeit und des Verhaltens der Arbeitnehmenden in vielen Fällen nicht nur zum Schutze ihrer eigenen Interessen berechtigt, sondern im Interesse der Öffentlichkeit oder anderer Arbeitnehmenden (Fürsorgepflicht) sogar verpflichtet. Kontrolle und Überwachung haben in den in Art. 328 und 328b OR, im DSG und im ArG verankerten Schranken stattzufinden. Zwei Aspekte sind hervorzuheben: Zum einen werden mit jeder Überwachung Personendaten der Arbeitnehmer/innen bearbeitet. Das hat zur Folge, dass Art. 328b OR und die (weiteren) Datenbearbeitungsgrundsätze des DSG eingehalten werden müssen. Zum anderen kommt in Art. 26 ArGV 3 der Grundgedanke zum Ausdruck, dass sich übermässige Überwachung negativ auf die Gesundheit der Arbeitnehmenden auswirkt. Im Lichte der neueren Bundesgerichtsrechtsprechung wird die Aussage in Art. 26 Abs. 1 ArGV 3, wonach eine (reine) Verhaltensüberwachung der Arbeitnehmenden per se die Gesundheit gefährde, etwas relativiert. Im Interesse der Rechtssicherheit ist zu prüfen, ob die Schranken der zulässigen Überwachung der Arbeitnehmenden nicht durch eine über Art. 6 ArG hinausgehende ausdrückliche gesetzliche Grundlage zu verankern wären.

---

50 ANTHONY BEM, Les Licenciements Facebook: évolution et dernières actualités jurisprudentielles, http://www.legavox.fr/blog/maitre-anthony-bem/«-licenciements-facebook-»-evolution-7765.htm (besucht: 17.5.2012).

IV) Spannungsfelder und Widersprüche

1. Datensammeln und Überwachen zum Schutze der Ethik?

Die Supermarktkette Wal Mart kennt weltweit Ethik-Richtlinien (Codes of Ethics), so auch für die Niederlassung in Deutschland. Der "Code of Ethics" enthält u.a. einen Drogentest bei Stellenantritt, ein Flirt- und Liebesverbot am Arbeitsplatz, ein Liebes- und Ausgehverbot mit Untergebenen oder Vorgesetzten im privaten Bereich, ein Verbot der privaten Internetnutzung. Zudem beinhaltet das Papier die Pflicht aller Mitarbeiter zur Meldung sämtlicher Verstösse von Kollegen gegen die Ethik-Regeln über eine anonyme Hotline, an einen Vorgesetzten oder an das Ethik-Büro[51]. Das Arbeitsgericht Wuppertal kommt zum Schluss, dass mehrere Bestimmungen des Codes gegen deutsches Recht verstossen, u.a. gegen Datenschutzregeln, das Grundgesetz und das Betriebsverfassungsgesetz[52]. Das Urteil wurde vom Landesarbeitsgericht Düsseldorf bestätigt[53].

Immer mehr Unternehmen führen so genannte Compliance- und Ethikrichtlinien ein. Hintergrund dieser Selbstgesetzgebung der Unternehmen bilden Bestimmungen der New York Stock Exchange (NYSE). Unternehmen, die hier kotiert sind, müssen bestimmte Corporate Governance Standards erfüllen, die in Abschnitt 303A des NYSE-Handbuchs für börsenkotierte Gesellschaften (NYSE Listed Company Manual) geregelt sind. Das Beispiel der Supermarktkette Wal Mart zeigt, dass global tätige Unternehmen ihre firmeninternen Vorschriften für das Verhalten der Arbeitnehmenden den nationalen Gesetzen anzupassen haben. Das gilt insbesondere auch für die heiklen Themenbereiche der Überwachung und Kontrolle der Arbeitnehmenden.

---

51 Die aktuelle Version des Walmart-Ethic-Codes findet sich hier: http://www.walmartstores.com/media/cdnpull/statementofethics/pdf/U.S_SOE.pdf (besucht: 19.5.2012).

52 http://www.justiz.nrw.de/nrwe/arbgs/duesseldorf/arbg_wuppertal/j2005/5_BV_20_05beschluss20050615.html (besucht: 19.5.2012).

53 http://www.iww.de/quellenmaterial/dokumente/053683.pdf (besucht: 19.5.2012).

2. Speicherung von Daten im Interesse des Datenschutzes?

Der Europäische Gerichtshof für Menschenrechte entschied in der Rechtssache I. gegen Finnland[54], dass der Staat zum wirksamen Schutz vor Verletzung des Rechts auf Privatleben (Art. 8 EMRK) es nicht dabei bewenden lassen kann, Rechtsbehelfe gegen Datenschutzverletzungen bereitzustellen, vielmehr muss der Staat durch geeignete Massnahmen dafür sorgen, dass die Datenschutzbestimmungen in der Praxis tauglich sind[55]. Sachverhalt der Entscheidung bildet die HIV-Infektion einer Mitarbeiterin eines Spitals, die gleichzeitig Patientin der Arbeitgeberin war. Die Beschwerdeführerin machte geltend, sie hätte ihre Stelle verloren, weil Vorgesetzte unbefugterweise Zugang zu ihren Patientendaten erhalten hätten. Vergeblich verlangte die Beschwerdeführerin von den zuständigen Verwaltungsbehörden, zu prüfen, wer unberechtigterweise ihre Patientenakte konsultiert hatte. Die Verantwortlichen des Spitals waren nicht in der Lage, diese Datenspur zu rekonstruieren. Das System erfasste in der fraglichen Zeitspanne lediglich die letzten fünf Zugriffe. So konnte die Beschwerdeführerin die Datenschutzverletzung nicht beweisen. Der Gerichtshof befand, dass im konkreten Fall die "log files" hätten aufbewahrt werden müssen. Bürgerinnen und Bürger müssen überprüfen können, ob Unbefugte Zugang zu ihren Personendaten hatten.

Paradoxerweise eröffnet diese Rechtsprechung auch ein Spannungsfeld: Effektiver Rechtsschutz gegen Datenverletzungen bedingt umfassendes Sammeln von Daten, was mit dem Gebot der schonenden Datenbearbeitung kollidieren kann.

---

54 EGMR vom 7. Juli 2008, Rechtssache I. gegen Finnland, Individualbeschwerde Nr. 20511/03.

55 EGMR vom 7. Juli 2008, Rechtssache I. gegen Finnland, Individualbeschwerde Nr. 20511/03, Rz 35. Siehe zum Urteil auch: KURT PÄRLI, EMRK und Datenschutz am Arbeitsplatz, Digma 1/2009, S. 30 ff.

3. Compliance – Freund oder Feind des Datenschutzes?

Ein Beispiel eines Widerspruchs zwischen firmeninternen Verhaltensvorschriften eines Konzerns und der nationalen Rechtsordnung wurde im weiter oben dargestellten Fall "Walmart" dargestellt. Spannungsfelder eröffnen sich auch bei den in den vergangenen Jahren zunehmend eingeführten Compliance-Regelungen. Unter Compliance ist vorab das an sich selbstverständliche Bekenntnis zur Einhaltung bestehender Gesetze und Verordnungen zu verstehen. Darüber hinaus umfasst die Compliance indes auch die Einhaltung von Branchen- und Unternehmensrichtlinien, die zum Teil die rechtlichen Vorgaben konkretisieren oder auch ergänzen. Als Treiber der Entwicklung in Richtung Ausbau von Compliance-Regelwerken wirken rechtliche Entwicklungen in den Bereichen Finanzmarktrecht, Korruptionsbekämpfung, Wettbewerbsrecht, Umweltschutzrecht, Schutz vor Belästigung, Diskriminierung.

Die Umsetzung von Compliance beruht im Wesentlichen auf drei Pfeilern[56]:

- Information und Sensibilisierung,
- Kontroll- und Überwachungsmassnahmen,
- Sanktionen gegen Regelverstösse.

Die Einhaltung des Datenschutzes bildet einen Aspekt der Compliance. Verstösse gegen Datenschutzvorschriften sind Rechtsverstösse und können straf-, zivil- und verwaltungsrechtliche Sanktionen nach sich ziehen. Darüber hinaus bergen Datenschutzverletzungen Reputationsrisiken.

Die Umsetzung von Compliance birgt indes auch die Gefahr von Datenschutzverletzungen. Die möglichen Problemfelder sind vielfältig:

- Unzulässige Beschaffung von Personendaten,
- unzulässige Datenverknüpfungen (Rasterfahndung),
- fehlender Einbezug der Arbeitnehmenden (Überwachung der Arbeitnehmenden erfordert deren Mitwirkung, da die Überwachung Auswirkungen auf die Gesundheit der Arbeitnehmenden haben kann).

---

56 DIRK FOX, Compliance und Datenschutz, in: DuD – Datenschutz und Datensicherheit 6/2008, S. 409 ff.

Die möglichen Widersprüche zwischen Compliance und Datenschutz lassen sich nur vermeiden, wenn bei der Implementierung von Compliance die datenschutzrechtlichen Grundsätze beachtet werden. Das kann auch bedeuten, dass nicht sämtliche Kontroll- und Überwachungsmassnahmen, die für eine möglichst hohe Compliance erforderlich wären, auch tatsächlich umgesetzt werden können. Die involvierten Akteure im Unternehmen sind hier gefordert, das richtige Mass zwischen Vertrauen und Kontrolle zu finden. Das gleiche Gebot ist auch dem Gesetzgeber mit auf den Weg zu geben, der die zunehmenden Compliance-Aktivitäten durch emsiges Legiferieren massgeblich gefördert hat und weiterhin fördert.

V) Fazit und weiterführende Überlegungen

Die Überwachung von Arbeitnehmenden ist allgegenwärtig. Das zeigen Skandale wie jüngst derjenige in der Supermarktkette Aldi, wonach sowohl Mitarbeitende wie auch Kunden (und vor allem Kundinnen) unrechtmässig gefilmt und überwacht worden sind[57]. Der Aldi-Datenskandal reiht sich ein in eine Reihe von Affären der letzten Jahre: So liess die Deutsche Bahn tausende von Mitarbeiter/innen zwecks Korruptionsbekämpfung systematisch überwachen, was gegen das Datenschutzrecht verstiess und zu einem Bussgeld von über einer Million Euro führte[58]. Verschiedene Firmen gerieten in Verruf, illegal Krankheitsdaten der Mitarbeitenden zu bearbeiten[59].

In den vorangehenden Ausführungen wurde deutlich, dass die Überwachung der Arbeitnehmenden auf verschiedenen Legitimationsgrundlagen beruht, die Arbeitgebenden sind häufig durch gesetzliche Regelungen verpflichtet, die Arbeit und das Verhalten ihrer Arbeitnehmenden zu kontrollieren. Da mit jeder Kontroll- und Überwachungstätigkeit Personendaten

57 Spiegelbericht: Aldi überwacht Mitarbeiter/innen – und Kunden/innen, http://www.spiegel.de/wirtschaft/unternehmen/0,1518,830372,00.html (besucht: 19.5.2012).

58 http://www.datenschutz-berlin.de/public/search (Stichwort "Deutsche Bahn" eingeben, führt danach zum Bussgeldentscheid), besucht: 19.5.2012.

59 http://www.hensche.de/Arbeitsrecht_aktuell_Krankheitsdaten_im_Muell_Datenspeicherung_bei_Lidl_Mercedes-Benz_Mueller.html (besucht: 19.5.2012).

der Arbeitnehmenden beschafft und (weiter-) bearbeitet werden, ist über die arbeitsrechtlichen Gesundheits- und Persönlichkeitsschutzbestimmungen des Arbeitsgesetzes hinaus immer auch das Datenschutzrecht einschlägig.

Nimmt man die Anzahl der Gerichtsentscheide zu individualrechtlichen Klagen gegen Datenschutzverletzung als Indikator für die Wirksamkeit des Datenschutzrechts, ist fraglich, ob die Gesetzgebung den beabsichtigten Zweck realisiert. Es gibt kaum erfolgreiche Klagen von Arbeitnehmenden gegen Datenschutzverletzungen. Abschreckend wirken Verfahrenshürden. Eine Datenschutzverletzung muss von den Arbeitnehmenden bewiesen werden. Dazu kommt das Kostenrisiko eines Prozesses. Darüber hinaus besteht das eminent praktische Problem, dass bei einem gerichtlichen Vorgehen gegen eine Datenschutzverletzung genau die Information (erneut) zum Thema gemacht werden muss, die von der betroffenen Person gerade hätte geheim gehalten werden wollen[60]. Wenig zur praktischen Wirksamkeit des schweizerischen Datenschutzrechts tragen weiter die weitgehend fehlenden Sanktionen bei. Bussgelder in Millionenhöhe, wie sie die deutschen Datenschutzbehörden aussprechen können, kennt das schweizerische Datenschutzrecht nicht.

Vor diesem Hintergrund drängen sich Verbesserungen des geltenden Datenschutzrechts auf. Wünschbar ist auch eine erhöhte Sensibilisierung der Sozialpartner für die Datenschutzthemen. Normative Bestimmungen in Gesamtarbeitsverträgen könnten ein Mittel darstellen, um eine sinnvolle Begrenzung der Beschaffung und insbesondere auch der Verwertung von Arbeitnehmerpersonendaten vorzunehmen. Eine bessere Rechtsdurchsetzung im Bereich des arbeitsrechtlichen Datenschutzes liesse sich zudem durch eine Beweislasterleichterung bei Klagen wegen Verletzung von Art. 328 und 328b OR realisieren. Auch abschreckende Pönalentschädigungen, wie sie bei missbräuchlicher Kündigung vorgesehen sind, könnten ein adäquates Mittel zur Stärkung des Datenschutzrechts sein.

60 KURT PÄRLI, Datenschutz durch Selbstregulierung?, Digma 2/2011, S. 66 ff.